A Social Engineering Discussion about Privacy Attacks and Defences Considering Web Browsers and Social Networks

Denys A. Flores
National Polytechnic School, Department of Informatics and Computer Sciences (DIC), Quito, Ecuador
denys.flores@epn.edu.ec

Abstract— Social engineering is the human side of hacking involving deliberate actions to violate privacy by persuading an individual to disclose private information. On the other hand, even when technical hacking and social engineering techniques are viewed as two different threats, hackers use the technology available to create sophisticated privacy attacks, like the Man-In-The-Middle attack, by combining technical skills and psychological techniques. Hence, this article reviews previous work in the field of security and privacy, and explores the technical and psychological aspects of social engineering in order to discuss their implication in social-engineering-based privacy attacks and defences considering web browsers and social networks.

Keywords – social engineering; hacking; privacy; attack; defences; web browser; social network; MITM; man-in-the-middle

I. INTRODUCTION

Social engineering is a hacking technique to exploit human trust involving the manipulation of people’s emotions in order to make them disclose private information by means of deception strategies [1]; hence, it can be inferred that privacy attacks and social engineering are closely related. Conversely, even though Nyamsuren and Choi [2] consider social engineering and technical hacking as two different privacy threats, the evolution of technology (including web browsers and social networks) has been used by hackers to enrich their technical skills [3], and simultaneously, complement their traditional social engineering strategies in order to craft more complex and advanced privacy attacks [4].

Therefore, the purpose of this article is to discuss the social engineering aspects of privacy attacks considering not only the psychological, but also the technical skills behind them. Thus, in section (2), the relationship between privacy attacks and social engineering is discussed taking into account deception and trust.

In Section (3), advanced privacy attacks and defences involving social engineering are explained, considering web browsers and social networks.

Finally, conclusions are given considering possible challenges involving social engineering in the context of web browsers and social networks.

II. THE ROLE OF SOCIAL ENGINEERING IN PRIVACY ATTACKS

Social engineering is the psychological aspect of privacy attacks due to both people’s likelihood to be manipulated or deceived [3], and the ability of the social engineer to employ technical hacking to build trust in the victims [5].

A. Deception: The Psychology of Privacy Attacks

As stated by Mitnick and Simon [4], people’s weaknesses, like the lack of awareness to recognize and protect private information along with their tendency of being too confident, are the Achilles’ heel of any privacy protection scheme. Consequently, these inherent psychological vulnerabilities in people’s behaviour can be exploited by a hacker using social engineering in order to persuade a person to either disclose private information, or convince him/her to perform an action in order to get unauthorized access to physical repositories of private information [2]; e.g. a building, a server, a web site, etc.

Even though, there are some types of social engineering attacks [6], the most suitable techniques to deceive people, are impersonation [7] and false authorization [8].

First, impersonation is pretending to be a person eager for information or help via telephone, email, or instant messages [4]. In this scenario, the hacker deceives the victims by requesting urgent help to solve a specific issue whilst useful information is leaked during the conversation.

In contrast, fake authorization, even though it involves impersonation to get as much information as possible [9], it requires forging authority from high-skilled employees like managers, or company’s associates so that the victim can be manipulated by the attacker using power, fear, or intimidation [10]. The purpose in this scenario is pushing the victim to disclose private information by warning of consequences if the victim refuses to do so.

B. Building Trust by Using Technology in Privacy Attacks

Since the modern technology protects the attacker by means of distance and anonymity [3], privacy attacks have become faster and more hazardous [11]. Thus, in order to deviate as much computer security as possible, trust between the victim and the attacker can be built by using the following technical skills:

- Phishing: It involves obtaining private information from the victim via a fake web site [8]; e.g. fake banking web sites, fake e-commerce web sites, etc. In this scenario,
the attacker combines the technical attack with social engineering in order to impersonate a trusted party so that access to private information can be granted with apparent confidence.

• **Spam**: It exploits the victim’s curiosity via attachments in fraudulent e-mail or chat messages, the content of which may be viruses, or access to phishing web sites [12]. In this scenario, the attacker sometimes forges authority in order to get private information as soon as possible; e.g. receiving a fake email from the victims’ bank asking to renew their bank credentials using a phishing web, and at the same time, warning about potential loss of funds if this is not done quickly.

• **Spoofing** [13]: this technique involves either IP Spoofing, or ARP injection. The first redirects the victim to a fake server in order to get unauthorized access to the victim’s computer; meanwhile, ARP injection exploits the lack of authentication in ARP packets so that the attacker can intercept, and manipulate a valid ARP Response Message to redirects the victim’s computer to a malicious server in a trusted communication [14].

To sum up, these examples are effective social engineering techniques to build trust in people because they may be combined to deceive the victim. For instance, an attacker may use spam to forge authority, and disseminate a phishing web site which impersonates a valid banking web site [13].

### III. ADVANCED PRIVACY ATTACKS AND DEFENCES CONSIDERING SOCIAL ENGINEERING

In this section, some relevant social-engineering-based privacy attacks against web browsers and social networks are discussed along with some privacy defence approaches to mitigate them.

#### A. Social-Engineering-Based Privacy Attacks against Web Browsers

In privacy attacks against web browsers, hackers exploit the victim’s trust so that unauthorized access to sensitive information can be gained by deviating the browser’s privacy protection. Particularly, the Man-In-The-Middle (MITM) attack is a dangerous social engineering approach using web browsers to obtain private information by inducing the victim to trust a party that claims to be legitimate [15]. In fact, a basic example of this attack can be performed by an insider using a key logger Trojan to impersonate a trusted party in order to leak the victim’s private information using Open Source tools available:

1. The windows/meterpreter/reverse_tcp payload of the metasploit framework available in the Linux Backtrack distribution can be used to create a key logger Trojan to impersonate a Windows 2003 Server critical update. The attack’s purpose is to deceive the victims making them believe that a critical update has to be downloaded to enhance the server performance.

2. The key logger is stored in the DocumentRoot path (fig. 1) specified in the httpd.conf file of the attacker’s Apache web server. In this example, the attacker’s web server’s IP address is 192.168.83.129.

![Figure 1. DocumentRoot path in the attacker’s Apache Web Server](image)

3. A simple fake web page (fig.2) is created to persuade the victims to download the suggested update, which seems to be critical. However, the victim ignores that this ‘update’ is a Trojan.

![Figure 2. Fake web page in the attacker’s machine](image)

4. Using the previous payload, the attacker’s machine has to be set as a fake DNS server (fig. 3).

   ![Figure 3. Setting up the attacker’s machine as a fake DNS Server](image)

In the payload, the IP address 192.168.83.129 is also the address of the fake DNS Server, which is also used to establish a reverse connection to spoof the keystrokes.

5. Via a silent ettercap session and ARP injection (fig. 4), all the valid DNS Requests from the victim’s web browser can be spoofed, and redirected to the fake DNS.

![Figure 4. DNS spoofing](image)

The generic command line for ettercap to perform this operation is:
errercap -i <ntw_ifce> -T -q -P dns_spoof /ip_add1/
/ip_add2/.../ip_addn/

Where:

- ntw_ifce is the network interface connected to the network to be spoofed
- -T specifies that the spoof attack will be done in text mode
- -q specifies that the attack will be performed in silent mode
- -P specifies the type of attack, in this case, dns_spoof

6. Once the victim uses the web browser, the attacker redirects the domain request to the fake DNS server. Since this server has a fake web server as well, the browser believes that the domain is valid, so it retrieves the fake web page instead of the real page that is hosted in the valid domain (fig. 5).

7. If the victim downloads the key logger, it will be installed as a background process; then, the attacker can capture all the victim’s keystrokes including passwords (fig. 6).

However, even though this attack seems simple under this approach, a powerful variant of the MITM attack can be performed against SSL sessions [16] to persuade the victims to trust a fake certificate in order to share a session key between the victim and the attacker (Chen et al., 2009, p.350); as consequence, the victims’ private information is shared with the attacker who can use it for malicious purposes.

Conversely, there are other social-engineered attacks targeting web browsers to exploit trust in the victims such as:

- **Search History Sniffing** [17]: In this attack, a hacker exploits a fake add-on to detect the frequency in which a web site is visited by manipulating the web site’s rendering so that its layout time can be simultaneously measured with the system clock in the victim’s computer.

- **Cross-site scripting (XSS)** [18]: Hackers employ this attack as an unauthorized form of code injection into the victim’s web browser using an untrusted web site; then, once the victim trusts the cross-scripted web site in the web browser, hackers can exploit the script to find their way around the victim’s computer and leak private information.

**B. Privacy Defences in Web Browsers**

Some defence mechanisms to protect web browsers against social-engineering-based privacy attacks are:

- **Browsing history defence** [17]: It is a mechanism that enables the web browser to pretend that all the web links in the search history were not visited; therefore, there is no difference between the times of visited and unvisited web sites. In addition, a variant of this defence [19] was suggested using a client/server camouflage so that each visited web site is replaced by a pseudonym in order to make it difficult for the attacker to guess which web sites were visited. However, this technique may cause a negative impact in the browsing experience and performance due to the conversion between the pseudonym and the real URL of the visited web site.

- **Access-Control-Based Web Browsers** [20]: This is a proposal of a new generation of web browsers to prevent history sniffing with an enhanced access control mechanism included in the browser’s kernel which seems to be an embedded firewall. Thus, the user can define access policies at plug-in level, configure the logs of visited web sites, and the allowance criteria for URLs according to access control policies.

- **Automatic-Detection-Security-Indicator** [16]: It is a novel web browser component to prevent MITM-based SSL attacks. It is based in the creation of a random indicator image to differentiate authentic web sites from fake ones. This random image is placed in a random place of the authentic web site so that an attacker cannot replicate neither the position nor the random image of the web site. Then, during SSL communications, the image and position is verified with a web site’s screenshot, if they do not match, a web spoofing alert is shown in the browser. Nonetheless, this process has to be done per SSL session which may increase the session overhead.

- **Cross-site scripting (XSS) detection** [18]: This is a content filtering mechanism which removes malicious scripts after the user input, avoiding hackers to inject arbitrary code in web sites via user-defined HTML content. Even though this mechanism could not be adopted due to standardization issues, an anti-XSS component compatible with current browsers was proposed. Then, only the insertion of benign user scripts is allowed by creating a blueprint representation of the user’s scripts using untrusted (client) and trusted (server) models. As a result, these models are parsed to detect
whether or not the client model intend to generate dangerous scripting calls into the server model.

C. Social-Engineering-Based Privacy Attacks against Social Networks

As stated by Oliveira et al. [21], as people’s interactions in social networks are based in trust, they are also likely to face social-engineered privacy attacks in order to capture personal information. In fact, there are ethical and social problems related to not only the social structures in social networks, but also the malicious exploitation of people interaction with technology [22]. Thus, in privacy attacks against social networks, hackers have as strategies the disclosure of consumer information [23], and the de-anonymization of personal profiles [24].

First, consumer information disclosure [23] is a dishonest way to get personal information from social networks which cannot be considered as a privacy attack if the associated disclosure event is not sanctioned by the law. Hence, the collection of personal information cannot be ethically limited, and sensitive data can be leaked for data mining, and advertisement purposes without the user consent [24].

Conversely, as stated by Luo and Lee [25], the de-anonymization of personal profiles implies the following combination of social engineering and technical hacking skills:

- **Out-of-context information disclosure**: It is the exploitation of people’s trust based on the victim’s over reliance on privacy protection tools offered by social networks. In fact, an attacker can exploit a bad configuration of privacy tools to get access to personal information using just search engines; in addition, since some tools in social networks are developed by insecure third-parties, the dissemination of malware through the social network is easier and faster once the victims have trusted the malicious tools [26]. As a result, the exploitation of trust using the flaws in social networks’ privacy tools is a very complex problem which is not just related to the victims, but also to privacy flaws in untrusted third-party tools in social networks.

- **In-Network information aggregation**: In social networks, impersonation is easier to perform by the attacker via false profiles, which are used to leak personal information to avoid face-to-face interactions, and the intervention of network administrators. In this scenario, the attacker just needs to get a friend invitation accepted in order to access to the victim’s friend list to either disseminate malicious content or collect their email addresses [27]. However, this attack is unlikely to be scalable due to the large number of active fake profiles required to harvest a large amount of users [24], so it may be more suitable when the target is a specific person, or a small number of users.

- **Cross-Network Information aggregation**: This form of attack can be performed by using data retrieval techniques to collect and analyze the overlapped information related to the same person across different social networks [25]. A case in point is the collaborative connection between social networks using integrated tools [27], e.g. Facebook and Twitter. Hence, once the victims have accepted the attacker as friend, the attacker can track and collect information of victims using their information in personal profiles in different, but related social networks, in order to craft and disseminate very personalized and believable spam [24].

D. Privacy Defenses in Social Networks

In the case of social networks, it is important to consider that anonymity is not enough for privacy protection [24], and even though the best way to protect sensitive information from privacy attacks is building user awareness and proper training [4], it may be very difficult to assure both considering the amount of users in social networks, e.g. Facebook has more than 800 million of active users [28]. Therefore, the solutions for privacy attacks in social networks to mitigate social engineering issues might consider the enhancement of the current user experience in the following aspects:

- **Implementation of socially-aware operative systems** [21]: This proposal involves a new generation of socially-aware operative systems with information detection: user’s behaviour detection models, and trust-aware system call interfaces in order to associate a level of trust depending on the social network interactions of each user. However, even when the proposal is very optimistic to control privacy, constraints related to user policies and information disclosure may be a problem, especially when social networks use marketing as main target of user exploitation, e.g. Facebook’s terms explicitly states that users’ profiles may be shared for the marketing purposes [24]. Therefore, these marketing interests in social network providers may cause constraints in their sponsors which can refrain the adoption of such operative systems.

- **Implementation of Privacy Information Disclosure Monitors** [25]: This privacy protection scheme is based on extracting the information from users registered in specific social networks by using retrieval techniques such as in-network and cross-network aggregation. Then, the information is organized and presented to the users so they can define an appropriate level of disclosure related to that information objects. Also, every time users share private information in any of their social networks, this privacy scheme sends a report to the user so that actions can be taken to define the level of disclosure in the just-added information. Nonetheless, the disadvantage in this approach may be the exposure of personal information in just one single repository of information which can be also exploited via social-engineered-based privacy attacks.

- **Privacy Attack Detection using Taxonomy-based attack tree analysis** [23]: As a science, taxonomy is the categorization or classification of things based on a predetermined system to create a conceptual framework for analysis, discussion, or information retrieval; therefore, in the context of web sites, including social networks, taxonomy is the hierarchy of information organization into categories and subcategories [29] [30]. In particular, if the content of social networks is
properly categorized, the sensitive information contained into these categories can be protected in a much better way against information disclosure by defining policies to devise social-engineering-based privacy attacks via spam or phishing. Therefore, this model proposes some straightforward steps (fig. 7) in order to define the taxonomies of the attacks, and define attack trees based on these taxonomies.

![Figure 7. Defining Privacy Attack Trees](image)

1. Choose a set of guidelines considering the scenario in which personal information is obtained by lawful means, and with the knowledge or consent of the owner.
2. Determine which guidelines promote the attack (negative), or if they refrain privacy breaches (positive). If negative go to (3), else go to (4).

In steps (3) and (4) consider the D’Morgan Law in discrete mathematics to build clauses using key words like lawful, trusted, and fair as Boolean variables.
3. Extract the relevant clauses.
4. Extract the relevant clauses and find the exception (negation). E.g. \((\neg X \land \neg Y) \iff \neg X \lor \neg Y\)
5. Use the extracted clauses in (3) and (4) to define the taxonomies or categories of privacy attacks.
6. Find the common principle in the clauses and group them.
7. Define the acts of deception as privacy attacks
8. Define the privacy attack trees based on the taxonomies found.

IV. CONCLUSIONS

- Social engineering is a privacy issue that cannot be solved entirely by means of software or hardware protections [5] due to the fact that hackers are using technical skills and psychological methods to craft more advanced privacy attacks. For example, MITM attacks use an effective attack model not only to intercept communications, but also to build trust in the victim.

- The psychology of privacy attacks is related to impersonation and false authorization which represents the main principles of social engineering. Then, privacy defences must be developed considering not only the technical factors, but also the mind tricks that can be used by a hacker to access private information.

- Although not as dangerous as the MITM attack, history sniffing [17] and cross-site scripting (XSS) [18] are attacks that may be exploited in the future to gain unauthorized access to private information because coding flaws will always be present in any program, or application [31]. Moreover, these attacks require less technical tricks that those employed in MITM attacks, so building trust in the victims using them may require less time as well. Then since this point of view, social engineering attacks against privacy have to be effective, but quick at the same time.

- The usage of social engineering techniques such as in-network and cross-network aggregation for attacks and defences (see section III-C) may lead to social and ethical issues considering that it is not yet accepted that the same technique to break into people’s privacy is used to prevent them. A case in point is the issues about the lack of ethical and moral boundaries in which hacking may be considered as a crime, or a security defence [32].

ACKNOWLEDGMENT

The author wishes to acknowledge the guidance and encouragement of Dr. George Theodorakopoulos of the Cardiff University, United Kingdom.

REFERENCES


